Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs	)	WC Docket No. 18-89
	)	
	)	

REPLY COMMENTS OF CTIA

Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Thomas K. Sawanobori
Senior Vice President, Chief Technology Officer

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 Sixteenth Street, NW, Suite 600
Washington, DC 20036
(202) 736-3200

July 2, 2018

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs	)	WC Docket No. 18-89
	)	
	)	

REPLY COMMENTS OF CTIA

CTIA respectfully submits these reply comments in response to the Federal Communications Commission's (Commission) Notice of Proposed Rulemaking (NPRM), *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*.[1]

I. INTRODUCTION AND SUMMARY

The record in response to the NPRM demonstrates that the wireless industry and the broader communications sector are committed to ensuring the security of the U.S. communications supply chain.[2] The record also makes clear that the global supply chain is a complex system of interdependent technologies and equipment.[3] These considerations lead to three specific conclusions that can be drawn from the record.

---

[1] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Notice of Proposed Rulemaking, WC Docket No. 18-89, FCC 18-42 (rel. Apr. 18, 2018).

[2] *See, e.g.*, CTIA Comments at 3-6; EchoStar Comments at 4; Motorola Comments at 1-2; NCTA – The Internet & Television Association Comments at 3-6 ("NCTA Comments"); Telecommunications Industry Association Comments at 5-8 ("TIA Comments"); WTA – Advocates for Rural Broadband Comments at 2.

[3] *See, e.g.*, CTIA Comments at 2-3; Puerto Rico Telephone Company, Inc. Comments at 2-5 ("PRTC Comments"); TIA Comments at 84; USTelecom Comments at 4;.

First, while policymakers are right to consider ways to secure the U.S. communications sector's supply chain against bad actors, any action in this particular proceeding should be thoroughly coordinated among federal government agencies with appropriate jurisdiction and expertise – including the multiple relevant supply chain security processes that are presently underway – as well as with the communications sector stakeholders who know this market best. The record further demonstrates that, given the rapidly evolving threat environment and necessity of timely, critically sensitive information about such threats, the Commission should derive key supply chain security decisions from broader processes led by the Department of Homeland Security (DHS), the federal government's Sector Specific Agency for both the communications and IT sectors.[4] Specifically, the Commission should not develop its own determinations of suppliers that pose a national security risk, but should instead align itself with the guidance from a DHS-led process informed by input from both industry stakeholders and the U.S. intelligence community.

Second, the record makes clear that the Commission should ensure that any input from government agencies and private sector stakeholders is appropriately protected. Consistent with CTIA's initial comments, the record supports the 2015 recommendation from the Commission's Communications Security, Reliability and Interoperability Council (CSRIC) that sensitive

[4] *See* Presidential Policy Directive – Critical Infrastructure Security and Resilience, PPD-21 (2013). *See also, e.g.,* Competitive Carriers Association Comments at 22 ("CCA Comments"); Computer & Communications Industry Association Comments at 6 ("CCIA Comments"); EchoStar Satellite Operating Corporation, Hughes Network Systems, LLC Comments at 7-8 ("EchoStar Comments"); NCTA Comments at 6-7; NTCA – The Rural Broadband Association Comments at 15 ("NTCA Comments"); PRTC Comments at 2-6; Rural Broadband Alliance Comments at 13 ("RBA Comments"); TIA Comments at 77-80; USTelecom Comments at 5.

private sector input to the government on critical issues of national security be afforded the statutory Protected Critical Infrastructure Information (PCII) protections administered by DHS.[5]

Third, largely due to the necessarily public nature of this proceeding, there is a lack of clarity and consensus in the record regarding the costs and benefits of the Commission's proposed action. This simply reinforces the need for the Commission to work with other expert agencies to conduct a thorough quantitative and qualitative analysis of the costs and benefits of various approaches before taking action that will likely have significant effects throughout the communications and IT sectors.[6]

II. THE RECORD MAKES CLEAR THAT THE COMMISSION SHOULD DERIVE KEY SUPPLY CHAIN SECURITY DECISIONS FROM BROADER INTERAGENCY PROCESSES LED BY DHS, WITH PCII PROTECTIONS FOR PRIVATE SECTOR INPUT

Consistent with CTIA's initial comments, the record demonstrates that any action the Commission might consider taking as part of this proceeding should derive from well-coordinated efforts among federal government agencies with the requisite experience, information, and resources to address national security and supply chain risk management.[7] Further, the Commission's notice-and-comment rulemaking process is neither agile nor flexible enough to keep up with the rapid pace of changing policy and market dynamics implicated by

[5] *See, e.g.*, CTIA Comments at 18-19; NCTA Comments at 11-12; TIA Comments at 81; USTelecom Comments at 10-11.

[6] *Compare* TIA Comments at 66-77 *with* CCA Comments at 29-34 *and* Sagebrush Cellular, Inc. Comments at 2-4 ("Sagebrush Comments").

[7] *See, e.g.*, CCA Comments at 22; CCIA Comments at 6; EchoStar Comments at 7-8; NCTA Comments at 6-7; NTCA Comments at 15; PRTC Comments at 2-6; RBA Comments at 13; TIA Comments at 77-80; USTelecom Comments at 5.

national security considerations.[8] For this reason, any Commission action should fully align with, and be sufficiently flexible to accommodate, broader interagency efforts and pending statutory developments.

The record clearly demonstrates that the Commission should rely upon the expertise of other agencies, such as DHS. As NCTA notes, "DHS, the Sector Specific Agency for both the communications and the IT sectors, plays a key role in coordinating Federal agency efforts on cybersecurity, including supply chain security, and is well-positioned to coordinate the government's interagency efforts on these matters."[9] DHS is the government partner for the Communications Sector Coordinating Council (CSCC),[10] the sponsor of the National Security Telecommunications Advisory Council (NSTAC),[11] and the host of both the National Cybersecurity and Communications Integration Center (NCCIC)[12] and the co-located National Coordinating Center for Communications (NCC) and its partners in the Communications Information Sharing and Analysis Center (Comm ISAC).[13] These longstanding institutions are the primary institutional partnerships between the communications sector and the government on all matters of cybersecurity policy and operations, and thus they and DHS should be at the center

[8] *See* USTelecom Comments at 10.

[9] NCTA Comments at 7; *see also* CCA Comments at 22; EchoStar Comments at 7-8; TIA Comments at 81; USTelecom Comments at 10-12.

[10] *See* CTIA Comments at 5.

[11] *See* CTIA Comments at 6.

[12] *See* Department of Homeland Security, *National Cybersecurity and Communications Integration Center*, https://www.us-cert.gov/nccic.

[13] *See* CTIA Comments at 6.

of any government effort – including any Commission action in this proceeding – to advance supply chain security.[14]

Further, as CTIA noted in its initial comments, only DHS has the statutory authority to appropriately protect the confidentiality of the critically sensitive information that would be necessary to fully evaluate supply chain risks. The record confirms that the Commission's protective order governing the submission and review of confidential information in this proceeding is not sufficient to address confidentiality concerns. Simply put, a Commission-issued protective order cannot provide the same level of protections and certainty that DHS's statutory PCII protections provide,[15] such as guarantees that information will not be publicly disclosed – including under the Freedom of Information Act or similar State, local, tribal, or territorial disclosure laws – and will not be used in civil litigation, enforcement actions, or for regulatory rulemaking purposes.[16] Therefore, the Commission should follow CSRIC's 2015 recommendation that private sector input to the government on such critical and sensitive topics should be afforded the statutory PCII protections administered by DHS.[17] As USTelecom notes, "the purpose of the PCII program is to better enable collaboration" between the private sector and government, and PCII protections will allow industry to "feel more confident in participating in a process that necessarily involves divulging very sensitive information about potential

[14] *See* EchoStar Comments at 7-8; NCTA Comments at 7-8; TIA Comments at 81; USTelecom Comments at 10-14.

[15] *See* CTIA Comments at 19; NCTA Comments at 11-12; USTelecom Comments at 11-12.

[16] *See* Procedures for Handling Critical Infrastructure Information, Final Rule, 6 C.F.R. § 29.3 (2006).

[17] *See* NCTA Comments at 3; TIA Comments at 81; USTelecom Comments at 11-12.

vulnerabilities in their products."[18] The Commission should rely primarily on DHS for information about communications sector supplier and supply chain risks because DHS will have the most insightful private sector information protected by PCII, as well as the U.S. government's classified intelligence information and related analysis.

Overall, the record demonstrates that the Commission should not develop its own determinations of specific suppliers that pose a national security risk. The U.S. Government should speak with one voice on these matters, and DHS has already been designated as the lead agency. Acting on its own, the Commission does not have the expertise, information, or resources necessary to develop and publish a list of its own independent determinations, or to maintain and update such a list in a quickly evolving threat environment.[19] The record demonstrates that Commission designations should instead be derivative of other authorities' determinations.[20] To the extent that the Commission decides to play a role in clarifying to USF recipients the names or descriptions of restricted or prohibited suppliers, such designation should only publicize other authorities' previous determinations for the purpose of clear notice to USF recipients.[21] Given the quickly evolving threat landscape, the names and/or descriptions of such

[18] *See* USTelecom Comments at 12.

[19] *See* CCA Comments at 5; CCIA Comments at 6; EchoStar Comments at 7-8; NCTA Comments at 7-10; NTCA Comments at 22-23; TIA Comments at 55-60; USTelecom Comments at 8-10.

[20] *See, e.g.*, Motorola Comments at 3-4; NCTA Comments at 7-10; TIA Comments at 55-60; USTelecom Comments at 8-10.

[21] *See* NCTA Comments at 7-10; TIA Comments at 55-60; USTelecom at 8-10.

entities should not be codified in the Commission's rules, such that a change would require another notice-and-comment rulemaking process.[22]

III. THE RECORD CONFIRMS THAT THE COMMISSION SHOULD WORK WITH EXPERT STAKEHOLDERS IN GOVERNMENT AND INDUSTRY TO CONDUCT A THOROUGH QUALITATIVE AND QUANTITATIVE COST-BENEFIT ANALYSIS BEFORE TAKING ACTION TO ADDRESS SUPPLY CHAIN SECURITY RISKS WITHIN THE FEDERAL USF PROGRAMS

While the NPRM focuses on actions within the federal USF programs, any Commission action in this proceeding will likely have significant ripple effects throughout the communications and IT sectors. As TIA observes, Commission action on supply chain risks in USF programs would be the first such rulemaking in either sector.[23] Through its decisions here, the Commission thus may set a precedent among other government agencies – or even a future Commission – for further supply chain requirements outside the USF setting. With the knowledge that other agencies may look to it for guidance, the Commission should take an approach that can serve as a model for robust and well-coordinated qualitative and quantitative analysis of costs and benefits of any government restrictions on certain suppliers.

The diversity of opinions and assertions in the record suggest that there is a need for the Commission, in consultation with DHS and other agencies, to ensure that the proposals in the NPRM are subject to a thorough and careful evaluation of the associated costs and benefits.[24] With regard to the quantifiable impact of Commission action, some commenters highlight that wireless carriers participating in the USF programs, as well as their customers, may face high

[22] *See* TIA Comments at 60-62; USTelecom Comments at 8-9.

[23] *See* TIA Comments at 3.

[24] *Compare* TIA Comments at 66-77 *with* CCA Comments at 29-34 *and* Sagebrush Comments at 2-4.

implementation costs and ongoing compliance costs should the Commission implement its proposed rule.[25] Conversely, some comments suggest that a competitively neutral and non-discriminatory approach could in fact preserve the competitive marketplace with negligible cost impact.[26] Commenters' reluctance to share sensitive information in a public proceeding may contribute to the somewhat equivocal state of the record. In any event, the record yields no definitive conclusions regarding the extent and scope of quantifiable costs and benefits of the proposed Commission action. A more thorough analysis of those costs and benefits, conducted in a context that protects sensitive and proprietary information, would provide a more reliable basis for Commission action.

Likewise, the record lacks clarity regarding the extent and nature of the qualitative, non-quantifiable impact of Commission action in this context. Indeed, there may be certain consequences for national security, among other considerations, that are difficult to measure. Those costs and benefits, however, would be best identified and evaluated in collaborative interagency processes that include appropriate national security and intelligence agencies. For example, the long-term national security and competitive impacts of Commission action in this proceeding could possibly be beneficial in accelerating the development of the competitive marketplace for trusted suppliers by sending a signal about the future importance of supply chain security; conversely, Commission action could potentially have the inadvertent effect of increasing supply chain risks if entities participating in the federal USF programs are faced with uncertainty over which suppliers are likely to be permitted over the long-term, thereby inhibiting

[25] *See, e.g.,* PRTC Comments at 6-7, Pine Belt Cellular, Inc. Comments at 5-7.

[26] *See, e.g.* TIA Comments at 71-77.

investment in secure equipment. The record is not clear on these points, because no deep fact-gathering or analysis has yet been undertaken.

This proceeding provides an opportunity for the government and pertinent market stakeholders to work together to develop the data and analysis necessary to weigh the costs and benefits of Commission action. A number of forthcoming efforts will further the Commission's, industry's, and the public's understanding of supply chain risks and the potential effects of any restrictions or prohibitions. For example, the Commission has directed the CSRIC to focus on supply chain risks for 5G, with a report due in September 2018.[27] In addition, DHS's Telecommunications Supply Chain Risk Assessments should advance the understanding of the complex considerations pertinent to these supply chain decisions.[28] Collectively, along with the record in this proceeding, these efforts may provide a basis of facts and data sufficient to begin the national security and market analysis that is necessary before the Commission acts in this proceeding.

Similarly, as CTIA stated in its initial comments, ascertaining the differing levels of risk of various equipment and network/device functions, and the various industry and government approaches that may best be able to address those differing risks, is not well-suited for prescriptive regulations from a single agency. As CTIA explained, the determination of where to draw the line between equipment that does or does not pose an actionable risk is a highly complex exercise that requires a process that permits diverse input, extensive collaboration, and

[27] *See* CSRIC VI Working Group Descriptions, at 3 (Mar. 14, 2018), *available at* https://www.fcc.gov/files/csric6wgdescriptions3-2018docx.

[28] *See* Department of Homeland Security, National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis, *Telecommunications Supply Chain Risk Assessments* (presentation of May 7, 2018).

adequate confidentiality protections.[29] Thus, decisions about supply chain risks should be made through a process coordinated by DHS that includes the many other agencies that regularly balance the competing equities and sensitive intelligence, as well as the diplomatic consequences of designations as other countries react to U.S. government action. With regard to the details of supply chain risk management pertaining to specific suppliers of various equipment and services, the record does not currently provide sufficient qualitative or quantitative inputs necessary to determine whether the overall impact of Commission action will result in benefits that outweigh the costs. This is another reason the Commission should work with expert stakeholders in government and industry to study the costs and benefits of various proposed restrictions and prohibitions prior to taking any final action in this proceeding.

IV. CONCLUSION

For the foregoing reasons, the record demonstrates that Commission should approach any final decision in this proceeding cautiously and with an emphasis on coordination with other expert agencies.

Respectfully submitted,

/s/ Melanie K. Tiano

Melanie K. Tiano
Director, Cybersecurity and Privacy

Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

[29] *See* CTIA Comments at 16-17.

Thomas K. Sawanobori
Senior Vice President, Chief Technology Officer

CTIA
1400 Sixteenth Street, NW, Suite 600
Washington, DC 20036
(202) 785-0081

July 2, 2018